(i)

1. **What should Alice transmit to Bob assuming we are restricted to public key cryptosystems? Use the notation above.**

Alice encrypts using bobs public key and sends the following to bob:

EPu(B)(M)

Bob decrypt using his private key

M = DPr(B)(EPu(B)(M))

1. **When large messages must be encrypted, symmetric key cryptography is usually preferred to public key cryptography. Explain why.**

Symmetric key cryptography is preferred for encrypting large messages because its much faster and more efficient than public keys(asymmetric) cryptography like RSA.

* Symmetric cryptography
* Very fast
* Small Keys
* Light weight resource usage
* Best used for bulk data encryption
* Public key cryptography
* Slower, involves larger prime math
* Larger keys
* CPU intensive
* Best used for key exchange and digital signatures

Public keys encryption is computationally expensive, making it inefficient for encryption large messages.

Symmetric algorithms are much faster, so are typically used for bulk encryption, while public key cryptography is better for key and signature exchanges

(ii)

1. **What should Alice transmit to Bob, to enable Bob to verify that it was indeed Alice who sent the message. Use the notation above. Do not worry about computational efficiency concerns.**

Alice encrypts the message with her private key:

S = EPr(A)(M)

Bob decrypts with Alices public key:

M = DPu(A)(S)

1. **If computational efficiency is a concern, what should Alice transmit to Bob to enable him to verify it was Alice who sent the message? Use public key cryptography along with other mechanisms as appropriate**

Alice computes a secure hash of the message:

H(M)

Then encrypts that hash with her private key to crate digital signature:

Sig = EPr(A)(H(M))

She sends:

(M,Sig) = (M(EPr(A)(H(M))

Bob receives M and Sig

H(M)

Decrypts the signature with Alices public key:

DPu(A)(Sig) = H(M’)

If:

H(M’) == H(M)

Then the message is authentic